70-744.exam.70q

Number: 70-744
Passing Score: 800
Time Limit: 120 min

70-744

Securing Windows Server 2016

Exam A

QUESTION 1

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated
goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains multiple Hyper-V hosts.

You need to deploy several critical line-of-business applications to the network to meet the following requirements:

- The resources of the applications must be isolated from the physical host.
- Each application must be prevented from accessing the resources of the other applications.
- The configurations of the applications must be accessible only from the operating system that hosts the application.

Solution: You deploy a separate Windows container for each application.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/

QUESTION 2

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains multiple Hyper-V hosts.

You need to deploy several critical line-of-business applications to the network to meet the following requirements:

- The resources of the applications must be isolated from the physical host.
- Each application must be prevented from accessing the resources of the other applications.
- The configurations of the applications must be accessible only from the operating system that hosts the application.

Solution: You deploy a separate Hyper-V container for each application.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/

QUESTION 3

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains multiple Hyper-V hosts.

You need to deploy several critical line-of-business applications to the network to meet the following requirements:

- The resources of the applications must be isolated from the physical host.
- Each application must be prevented from accessing the resources of the other applications.

- The configurations of the applications must be accessible only from the operating system that hosts the application.

Solution: You deploy one Windows container to host all of the applications.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/

QUESTION 4
Your network contains an Active Directory domain named contoso.com. The domain contains 1,000 client computers that run Windows 10.

A security audit reveals that the network recently experienced a Pass-the-Hash attack. The attack was initiated from a client computer and accessed Active Directory objects restricted to the members of the Domain Admins group.

You need to minimize the impact of another successful Pass-the-Hash attack on the domain.

What should you recommend?

A. Instruct all users to sign in to a client computer by using a Microsoft account.
B. Move the computer accounts of all the client computers to a new organizational unit (OU). Remove the permissions to the new OU from the Domain Admins group.
C. Instruct all administrators to use a local Administrators account when they sign in to a client computer.
D. Move the computer accounts of the domain controllers to a new organizational unit (OU). Remove the permissions to the new OU from the Domain Admins group.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:
https://en.wikipedia.org/wiki/Pass_the_hash#Mitigations

QUESTION 5
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2016.

You create a new bastion forest named admin.contoso.com. The forest functional level of admin.contoso.com is Windows Server 2012 R2.

You need to implement a Privileged Access Management (PAM) solution.

Which two actions should you perform? Each correct answer presents part of the solution.

A. Raise the forest functional level of admin.contoso.com.
B. Deploy Microsoft Identify Management (MIM) 2016 to admin.contoso.com.
C. Configure contoso.com to trust admin.contoso.com.
D. Deploy Microsoft Identity Management (MIM) 2016 to contoso.com.
E. Raise the forest functional level of contoso.com.
F. Configure admin.contoso.com to trustcontoso.com.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/hardware-software-requirements https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/planning-bastion-environment

QUESTION 6
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016.

Server1 is configured as a domain controller.

You configure Server1 as a Just Enough Administration (JEA) endpoint. You configure the required JEA rights for a user named User1.

You need to tell User1 how to manage Active Directory objects from Server2.

What should you tell User1 to do first on Server2?

A. From a command prompt, runntdsutil.exe.

B. From Windows PowerShell, run the Import-Module cmdlet.
C. From Windows PowerShell, run the Enter-PSSession cmdlet.
D. Install the management consoles for Active Directory, and then launch Active Directory Users and Computers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://blogs.technet.microsoft.com/privatecloud/2014/05/14/just-enough-administration-step-by-step/

QUESTION 7
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.

You deploy the Local Administrator Password Solution (LAPS) to the network.

You deploy a new server named FinanceServer5, and join FinanceServer5 to the domain.

You need to ensure that the passwords of the local administrators of FinanceServer5 are available to the LAPS administrators.

What should you do?

A. On FinanceServer5, register AdmPwd.dll.
B. On FinanceServer5, install the LAPS Windows PowerShell module.
C. In the domain, modify the permissions for the computer account of FinanceServer5.
D. In the domain, modify the permissions of the Domain Controllers organizational unit (OU).

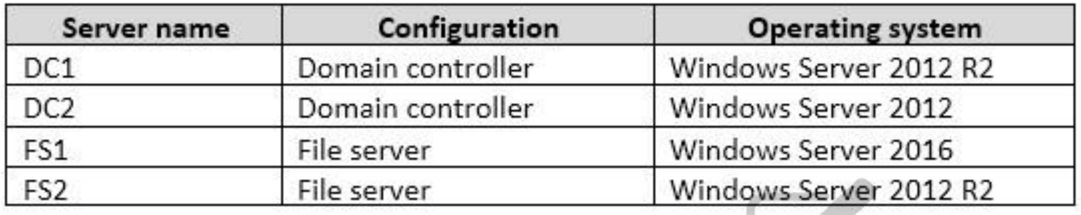
Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:
https://gallery.technet.microsoft.com/Step-by-Step-Deploy-Local-7c9ef772

QUESTION 8
Your network contains an Active Directory domain named contoso.com. The domain contains four servers. The servers are configured as shown in the following table.



Server name	Configuration	Operating system
DC1	Domain controller	Windows Server 2012 R2
DC2	Domain controller	Windows Server 2012
FS1	File server	Windows Server 2016
FS2	File server	Windows Server 2012 R2

You need to manage FS1 and FS2 by using Just Enough Administration (JEA).

What should you do before you can implement JEA?

A. Install Microsoft.NET Framework 4.6.2 on FS2.
B. Install Microsoft.NET Framework 4.6.2 on FS1.
C. Install Windows Management Framework 5.0 on FS2.
D. Upgrade DC1 to Windows Server 2016.

Correct Answer: C
Section: (none)
Explanation

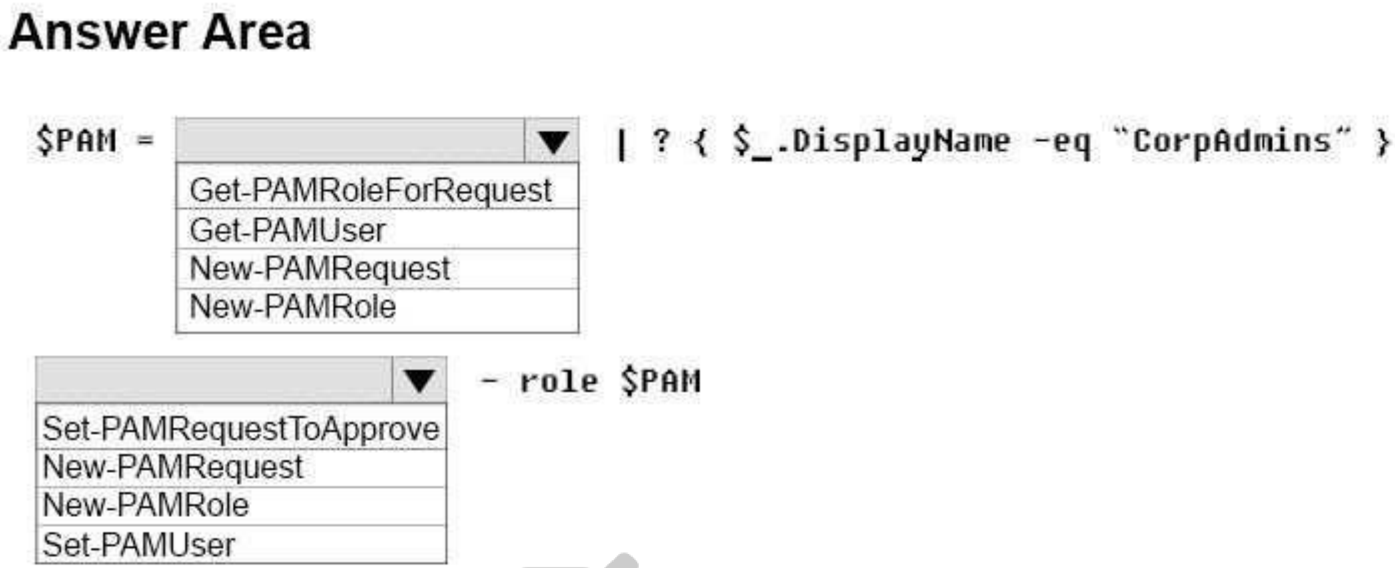
Explanation/Reference:
Explanation:

References: https://blogs.technet.microsoft.com/privatecloud/2014/05/14/just-enough-administration-step-by-step/

QUESTION 9
HOTSPOT

Your network contains an Active Directory forest named contoso.com.
The forest has Microsoft Identity Manager (MIM) 2016 deployed.
You implement Privileged Access Management (PAM).
You need to request privileged access from a client computer in contoso.com by using PAM.
How should you complete the Windows PowerShell script? To answer, select the appropriate options in the answer area.

Hot Area:

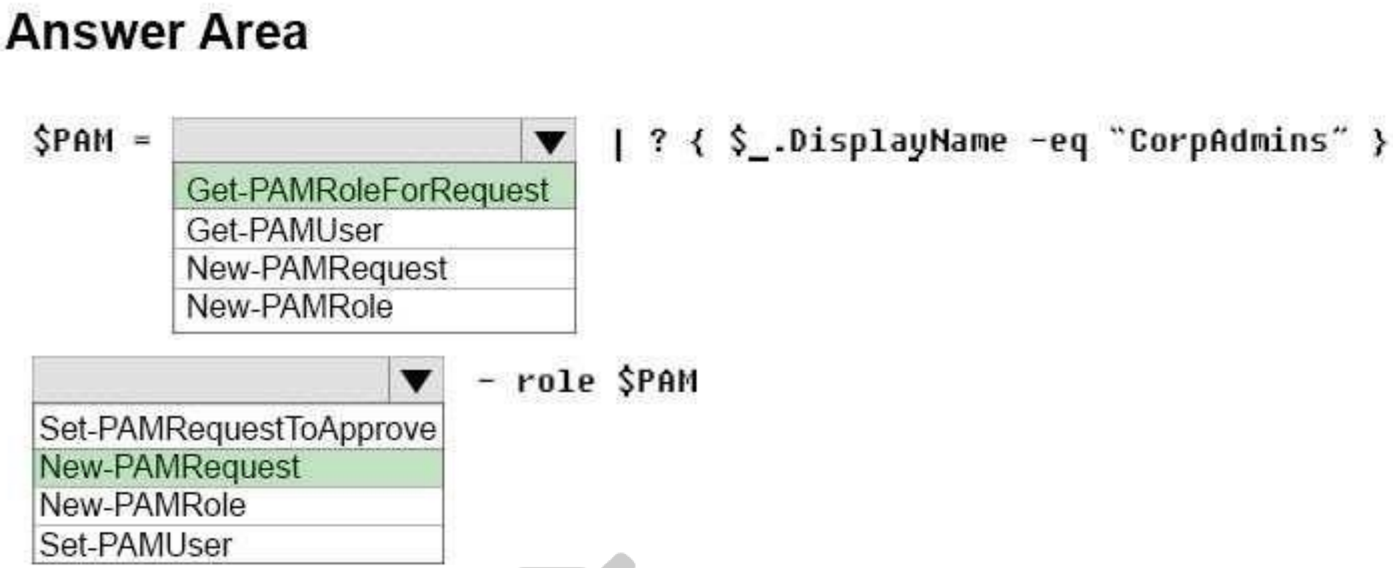


Answer Area

```
$PAM =                          | ? { $_.DisplayName -eq “CorpAdmins” }

                        - role $PAM
```

Correct Answer:



Answer Area

```
$PAM = ▼ | ? { $_.DisplayName -eq “CorpAdmins” }
```

[✓ Get-PAMRoleForRequest]
Get-PAMUser
New-PAMRequest
New-PAMRole

```
▼ - role $PAM
```

Set-PAMRequestToApprove
[✓ New-PAMRequest]
New-PAMRole
Set-PAMUser

Section: (none)
Explanation

Explanation/Reference:
References:
https://technet.microsoft.com/en-us/library/mt604089.aspx https://technet.microsoft.com/en-us/library/mt604084.aspx

QUESTION 10
Your network contains an Active Directory domain named contoso.com. The domain contains five servers. All servers run Windows Server 2016.

A new security policy states that you must modify the infrastructure to meet the following requirements: ▪
Limit the rights of administrators.
▪ Minimize the attack surface of the forest.
▪ Support Multi-Factor authentication for administrators.

You need to recommend a solution that meets the new security policy requirements.

What should you recommend deploying?

A. an administrative forest
B. domain isolation
C. an administrative domain in contoso.com
D. the Local Administrator Password Solution (LAPS)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material#ESAE_BM

QUESTION 11
Your network contains two single-domain Active Directory forests named contoso.com and contosoadmin.com. Contosoadmin.com contains all of the user accounts used to manage the servers in contoso.com.

You need to recommend a workstation solution that provides the highest level of protection from vulnerabilities and attacks.

What should you include in the recommendation?

A. Provide a Privileged Access Workstation (PAW) for each user account in both forests. Join each PAW to the contoso.com domain.
B. Provide a Privileged Access Workstation (PAW) for each user in the contoso.com forest. Join each PAW to the contoso.com domain.
C. Provide a Privileged Access Workstation (PAW) for each administrator. Join each PAW to the contoso.com domain.
D. Provide a Privileged Access Workstation (PAW) for each administrator. Join each PAW to the contosoadmin.com domain.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

QUESTION 12
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server5 that has the Windows Server Update Services server role installed.

You need to configure Windows Server Update Services (WSUS) on Server5 to use SSL.

You install a certificate in the local Computer store.

Which two tools should you use? Each correct answer presents part of the solution.

A. Wsusutil
B. Netsh
C. Internet Information Services (IIS) Manager
D. Server Manager
E. Update Services

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/hh852346(v=ws.11).aspx#bkmk_3.5.ConfigSSL

QUESTION 13
Your network contains an Active Directory domain named contoso.com. The domain contains 1,000 client computers that run Windows 8.1 and 1,000 client computers that run Windows 10.

You deploy a Windows Server Update Services (WSUS) server. You create a computer group for each organizational unit (OU) that contains client computers. You configure all of the client computers to receive updates from WSUS.

You discover that all of the client computers appear in the Unassigned Computers computer group in the Update Services console.

You need to ensure that the client computers are added automatically to the computer group that corresponds to the location of the computer account in Active Directory.

Which two actions should you perform? Each correct answer presents part of the solution.

A. From Group Policy objects (GPOs), configure the Enable client-side targeting setting.

B. From the Update Services console, configure the Computers option.
C. From Active Directory Users and Computers, create a domain local distribution group for each WSUS computer group.
D. From Active Directory Users and Computers, modify the flags attribute of each OU.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:
https://technet.microsoft.com/en-us/library/dd252762.aspx https://technet.microsoft.com/en-us/library/cc720433(v=ws.10).aspx

QUESTION 14
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

Server1 has a volume named Volume1.

A central access policy named Policy1 is deployed to the domain.

You need to apply Policy1 to Volume1.

Which tool should you use?

A. File Explorer
B. Shared Folders
C. Server Manager
D. Disk Management
E. Storage Explorer

F. Computer Management
G. System Configuration
H. File Server Resource Manager (FSRM)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-a-central-access-policy--demonstration-steps-#BKMK_1.4

QUESTION 15
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

Server1 has a shared folder named Share1.

You need to encrypt the contents to Share1.

Which tool should you use?

A. File Explorer
B. Shared Folders
C. Server Manager
D. Disk Management
E. Storage Explorer
F. Computer Management
G. System Configuration
H. File Server Resource Manager (FSRM)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:
https://msdn.microsoft.com/en-us/library/dd163562.aspx

QUESTION 16
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

Server1 has a shared folder named Share1.

You need to ensure that all access to Share1 uses SMB Encryption.

Which tool should you use?

A. File Explorer
B. Shared Folders
C. Server Manager
D. Disk Management
E. Storage Explorer
F. Computer Management
G. System Configuration
H. File Server Resource Manager (FSRM)

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:
https://support.microsoft.com/en-za/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,windows-server-2008-r2,-windows-8,-and-windows-server-2012
https://blogs.technet.microsoft.com/filecab/2012/05/03/smb-3-security-enhancements-in-windows-server-2012/

QUESTION 17
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016 and a Nano Server named Nano1.

Nano1 has two volumes named C and D.

You are signed in to Server1.

You need to configure Data Deduplication on Nano1.

Which tool should you use?

A. File Explorer
B. Shared Folders
C. Server Manager
D. Disk Management
E. Storage Explorer
F. Computer Management
G. System Configuration
H. File Server Resource Manager (FSRM)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/hh831434(v=ws.11).aspx

QUESTION 18
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2016.

You need to create Work Folders on Server1.

Which tool should you use?

A. File Explorer
B. Shared Folders
C. Server Manager
D. Disk Management
E. Storage Explorer
F. Computer Management
G. System Configuration
H. File Server Resource Manager (FSRM)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References:
https://blogs.technet.microsoft.com/canitpro/2015/01/19/step-by-step-creating-a-work-folders-test-lab-deployment-in-windows-server-2012-r2/
https://technet.microsoft.com/en-us/library/dn265974(v=ws.11).aspx

QUESTION 19
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

Server1 has a volume named Volume1.

Dynamic Access Control is configured. A resource property named Property1 was created in the domain.

You need to ensure that Property1 is set to a value of Big for all of the files in Volume1 that are larger than 10 MB.

Which tool should you use?

A. File Explorer

B. Shared Folders C. Server Manager
D. Disk Management
E. Storage Explorer
F. Computer Management
G. System Configuration
H. File Server Resource Manager (FSRM)

Correct Answer: H
Section: (none)
Explanation

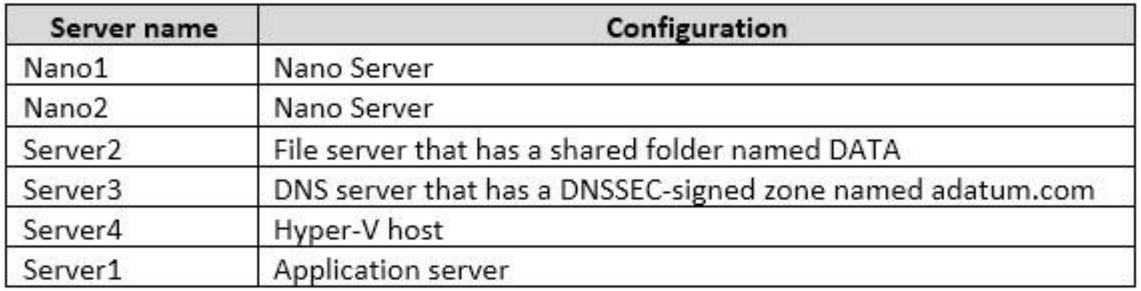
Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/cc732431(v=ws.11).aspx

QUESTION 20
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.

The domain contains the servers configured as shown in the following table.



Server name	Configuration
Nano1	Nano Server
Nano2	Nano Server
Server2	File server that has a shared folder named DATA
Server3	DNS server that has a DNSSEC-signed zone named adatum.com
Server4	Hyper-V host
Server1	Application server

All servers run Windows Server 2016. All client computers run Windows 10.

You have an organizational unit (OU) named Marketing that contains the computers in the marketing department. You have an OU named Finance that contains the computers in the finance department. You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU.

You install Windows Defender on Nano1.

You need to execute D:\Folder1 on Nano1 from being scanned by Windows Defender.

Which cmdlet should you run?

A. Set-StorageSetting
B. Set-FsrmFileScreenException
C. Set-MpPreference
D. Set-DtcAdvancedSetting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

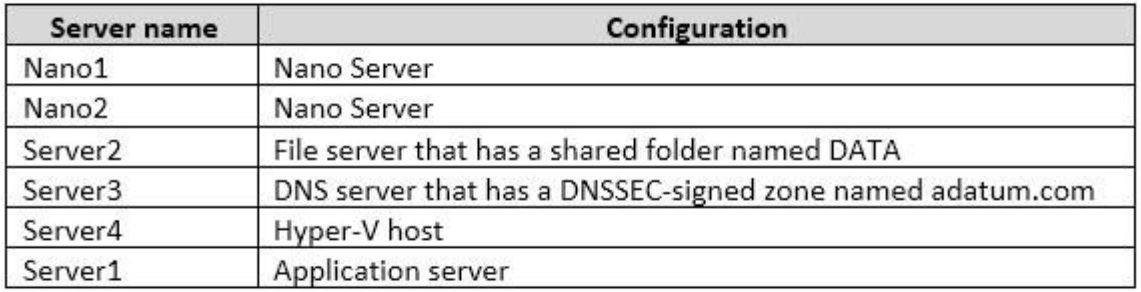
References: http://www.thomasmaurer.ch/2016/07/how-to-disable-and-configure-windows-defender-on-windows-server-2016-using-powershell/

QUESTION 21

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.

The domain contains the servers configured as shown in the following table.



Server name	Configuration
Nano1	Nano Server
Nano2	Nano Server
Server2	File server that has a shared folder named DATA
Server3	DNS server that has a DNSSEC-signed zone named adatum.com
Server4	Hyper-V host
Server1	Application server

All servers run Windows Server 2016. All client computers run Windows 10.

You have an organizational unit (OU) named Marketing that contains the computers in the marketing department. You have an OU named Finance that contains the computers in the finance department. You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU.

You install Windows Defender on Nano1.
You need to ensure that the marketing department computers validate DNS responses from adatum.com.

Which setting should you configure in the Computer Configuration node of GP1?

A. TCPIP Settings from Administrative Templates
B. Connection Security Rule from Windows Settings
C. DNS Client from Administrative Templates
D. Name Resolution Policy from Windows Settings

Correct Answer: D
Section: (none)
Explanation

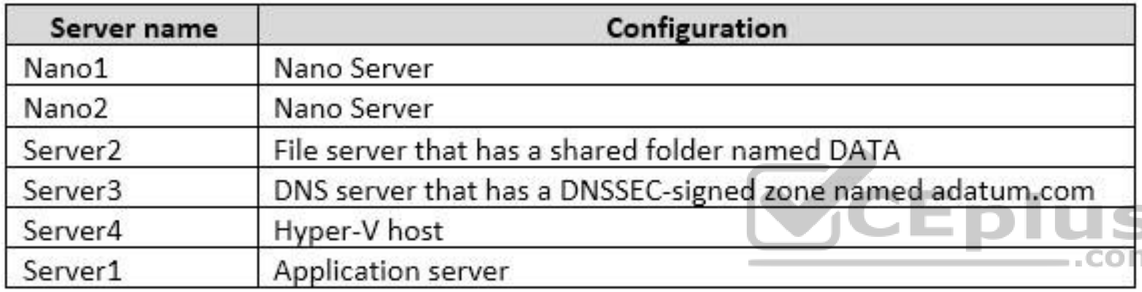
Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/ee649182(v=ws.10).aspx

QUESTION 22
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.

The domain contains the servers configured as shown in the following table.



Server name	Configuration
Nano1	Nano Server
Nano2	Nano Server
Server2	File server that has a shared folder named DATA
Server3	DNS server that has a DNSSEC-signed zone named adatum.com
Server4	Hyper-V host
Server1	Application server

All servers run Windows Server 2016. All client computers run Windows 10.

You have an organizational unit (OU) named Marketing that contains the computers in the marketing department. You have an OU named Finance that contains the computers in the finance department. You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU.

You install Windows Defender on Nano1.

You need to ensure that you can deploy a shielded virtual machine to Server4.

Which server role should you deploy?

A. Hyper-V
B. Device Health Attestation
C. Network Controller

D. Host Guardian Service

Correct Answer: D
Section: (none)
Explanation

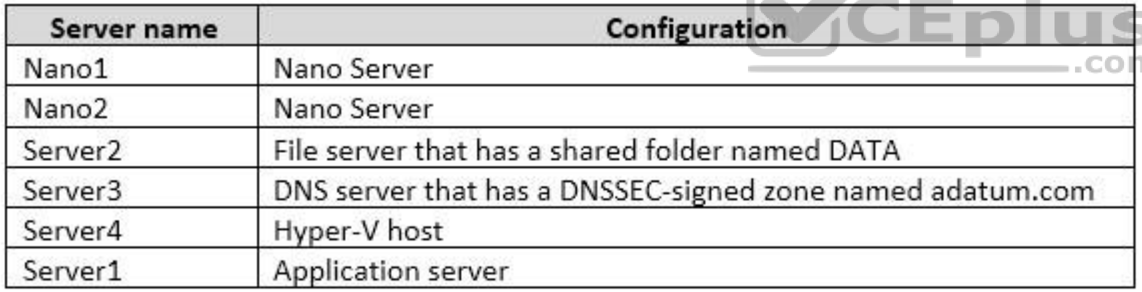
Explanation/Reference:
Explanation:

References: https://blogs.technet.microsoft.com/datacentersecurity/2016/03/16/windows-server-2016-and-host-guardian-service-for-shielded-vms/

QUESTION 23
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.

The domain contains the servers configured as shown in the following table.



Server name	Configuration
Nano1	Nano Server
Nano2	Nano Server
Server2	File server that has a shared folder named DATA
Server3	DNS server that has a DNSSEC-signed zone named adatum.com
Server4	Hyper-V host
Server1	Application server

All servers run Windows Server 2016. All client computers run Windows 10.

You have an organizational unit (OU) named Marketing that contains the computers in the marketing department. You have an OU named Finance that contains the computers in the finance department. You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU.

You install Windows Defender on Nano1.

You need to disable SMB 1.0 on Server2.

What should you do?

A. From File Server Resource Manager, create a classification rule.
B. From the properties of each network adapter on Server2, modify the bindings.
C. From Windows PowerShell, run the Set-SmbClientConfiguration cmdlet.
D. From Server Manager, remove a Windows feature.

Correct Answer: D
Section: (none)
Explanation

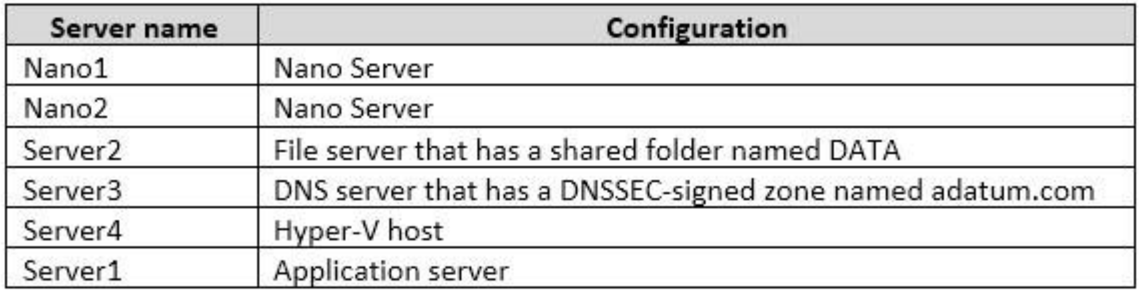
Explanation/Reference:
Explanation:

References: https://support.microsoft.com/en-za/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,windows-server-2008-r2,-windows-8,-and-windows-server-2012

QUESTION 24
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2.

The domain contains the servers configured as shown in the following table.



Server name	Configuration
Nano1	Nano Server
Nano2	Nano Server
Server2	File server that has a shared folder named DATA
Server3	DNS server that has a DNSSEC-signed zone named adatum.com
Server4	Hyper-V host
Server1	Application server

All servers run Windows Server 2016. All client computers run Windows 10.

You have an organizational unit (OU) named Marketing that contains the computers in the marketing department. You have an OU named Finance that contains the computers in the finance department. You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU.

You install Windows Defender on Nano1.

You plan to implement BitLocker Drive Encryption (BitLocker) on the operating system volumes of the application servers.

You need to ensure that the BitLocker recovery keys are stored in Active Directory.

Which Group Policy setting should you configure?

A. System cryptography: Force strong key protection for user keys stored on the computer
B. Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)
C. System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.
D. Choose how BitLocker-protected operating system drives can be recovered.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/jj679890(v=ws.11).aspx#BKMK_rec3

QUESTION 25
Your network contains an Active Directory domain named contoso.com.

You are deploying Microsoft Advanced Threat Analytics (ATA).

You create a user named User1.

You need to configure the user account of User1 as a Honeytoken account.

Which information must you use to configure the Honeytoken account?

A. The SAM account name of User1
B. The Globally Unique Identifier (GUID) of User1

C. the SID of User1
D. the UPN of User1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/working-with-detection-settings

QUESTION 26
Your network contains an Active Directory domain named contoso.com.

You create a Microsoft Operations Management Suite (OMS) workspace.

You need to connect several computers directly to the workspace.

Which two pieces of information do you require? Each correct answer presents part of the solution.

A. the ID of the workspace
B. the name of the workspace
C. the URL of the workspace
D. the key of the workspace

Correct Answer: AD

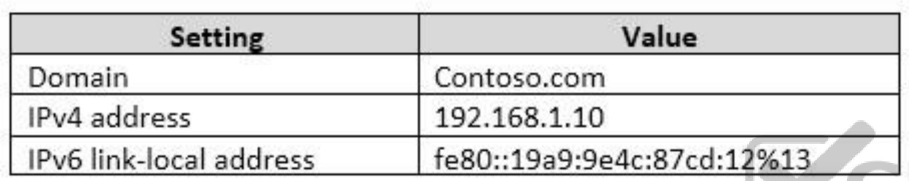
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents

QUESTION 27
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1.

Server1 is configured as shown in the following table.



Setting	Value
Domain	Contoso.com
IPv4 address	192.168.1.10
IPv6 link-local address	fe80::19a9:9e4c:87cd:12%13

You plan to create a pilot deployment of Microsoft Advanced Threat Analytics (ATA).

You need to install the ATA Center on Server1.

What should you do first?

A. Install Microsoft Security Compliance Manager (SCM).
B. Obtain an SSL certificate.
C. Assign an additional IPv4 address.D. Remove Server1 from the domain.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/install-ata-step1

QUESTION 28
Your network contains an Active Directory domain named contoso.com. The domain contains five file servers that run Windows Server 2016.

You have an organizational unit (OU) named Finance that contains all of the servers.

You create a Group Policy object (GPO) and link the GPO to the Finance OU.

You need to ensure that when a user in the finance department deletes a file from a file server, the event is logged. The solution must log only users who have a manager attribute of Ben Smith.

Which audit policy setting should you configure in the GPO?

A. File system in Global Object Access Auditing
B. Audit Detailed File Share
C. Audit Other Account Logon Events
D. Audit File System in Object Access

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://technet.microsoft.com/en-us/library/cc976403.aspx

QUESTION 29
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

You have an organizational unit (OU) named Administration that contains the computer account of Serve1.

You import the Active Directory module to Server1.

You create a Group Policy object (GPO) named GPO1. You link GPO1 to the Administration OU.

You need to log an event each time an Active Directory cmdlet is executed successfully from Server1.

What should you do?

A. From Advanced Audit Policy in GPO1, configure auditing for directory service changes.
B. Run the(Get-Module ActiveDirectory).LogPipelineExecutionDetails = $falsecommand.
C. Run the(Get-Module ActiveDirectory).LogPipelineExecutionDetails = $truecommand.
D. From Advanced Audit Policy in GPO1, configure for other privilege use events.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://www.petri.com/enable-powershell-logging

QUESTION 30
Your network contains an Active Directory domain named contoso.com.

You are deploying Microsoft Advanced Threat Analytics (ATA) to the domain.

You install the ATA Center on server named Server1 and the ATA Gateway on a server named Server2.

You need to ensure that Server2 can collect NTLM authentication events.

What should you configure?

A. the domain controllers to forward Event ID 4776 to Server2
B. the domain controllers to forward Event ID 1000 to Server1
C. Server2 to forward Event ID 1026 to Server1
D. Server1 to forward Event ID 1000 to Server 2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: http://winrook.blogspot.co.za/2015/12/configuring-windows-event-forwarding.html

QUESTION 31

Your network contains an Active Directory forest named contoso.com.

The network is connected to the Internet.

You have 100 point-of-sale (POS) devices that run Windows 10. The devices cannot access the Internet.

You deploy Microsoft Operations Management Suite (OMS).

You need to use OMS to collect and analyze data from the POS devices.

What should you do first?

A. Deploy Windows Server Gateway to the network.
B. Install the OMS Log Analytics Forwarder on the network.
C. Install Microsoft Data Management Gateway on the network.
D. Install the Simple Network Management Protocol (SNMP) feature on the devices.
E. Add the Microsoft NDIS Capture service to the network adapter of the devices.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

References: https://blogs.technet.microsoft.com/msoms/2016/03/17/oms-log-analytics-forwarder/

QUESTION 32

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You deploy Windows Server 2016 to a server named Server1.

You need to ensure that you can run Windows Containers on Server1.

Solution: On Server1, you enable the Containers feature, and then you install the PowerShell for Docker module. You restart the server.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/deploy-containers-on-server

QUESTION 33
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You deploy Windows Server 2016 to a server named Server1.

You need to ensure that you can run Windows Containers on Server1.

Solution: On Server1, you enable the Containers feature, and then you install the Hyper-V server role. You restart the server.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/deploy-containers-on-server

QUESTION 34

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You deploy Windows Server 2016 to a server named Server1.

You need to ensure that you can run Windows Containers on Server1.

Solution: On Server1, you enable the Containers feature, and then you restart the server.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/deploy-containers-on-server

QUESTION 35
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

You need to prevent NTLM authentication on Server1.

Solution: From a Group Policy, you configure the Security Options.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://www.rootusers.com/implement-ntlm-blocking-in-windows-server-2016/

QUESTION 36
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

You need to prevent NTLM authentication on Server1.

Solution: From Windows PowerShell, you run the **Disable-WindowsOptionalFeature** cmdlet.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://www.rootusers.com/implement-ntlm-blocking-in-windows-server-2016/

QUESTION 37
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

You need to prevent NTLM authentication on Server1.

Solution: From Windows PowerShell, you run the **New-ADAuthenticationPolicy** cmdlet.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://www.rootusers.com/implement-ntlm-blocking-in-windows-server-2016/

QUESTION 38
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2016.

Server1 has a shared folder named Share1.

You plan to create a subfolder in Share1 for each domain user.

You need to limit each user to using 100 MB of data in their respective subfolder. The solution must enable the users to be notified when they use 80 percent of the available space in the subfolder.

Which tool should you use?

A. File Explorer
B. Shared Folders
C. Server Manager
D. Disk Management
E. Storage Explorer
F. Computer Management
G. System Configuration
H. File Server Resource Manager (FSRM)

Correct Answer: H
Section: (none)
Explanation

Explanation/Reference:
References: https://4sysops.com/archives/file-server-resource-manager-fsrm-part-3-quota-management/

QUESTION 39
DRAG DROP

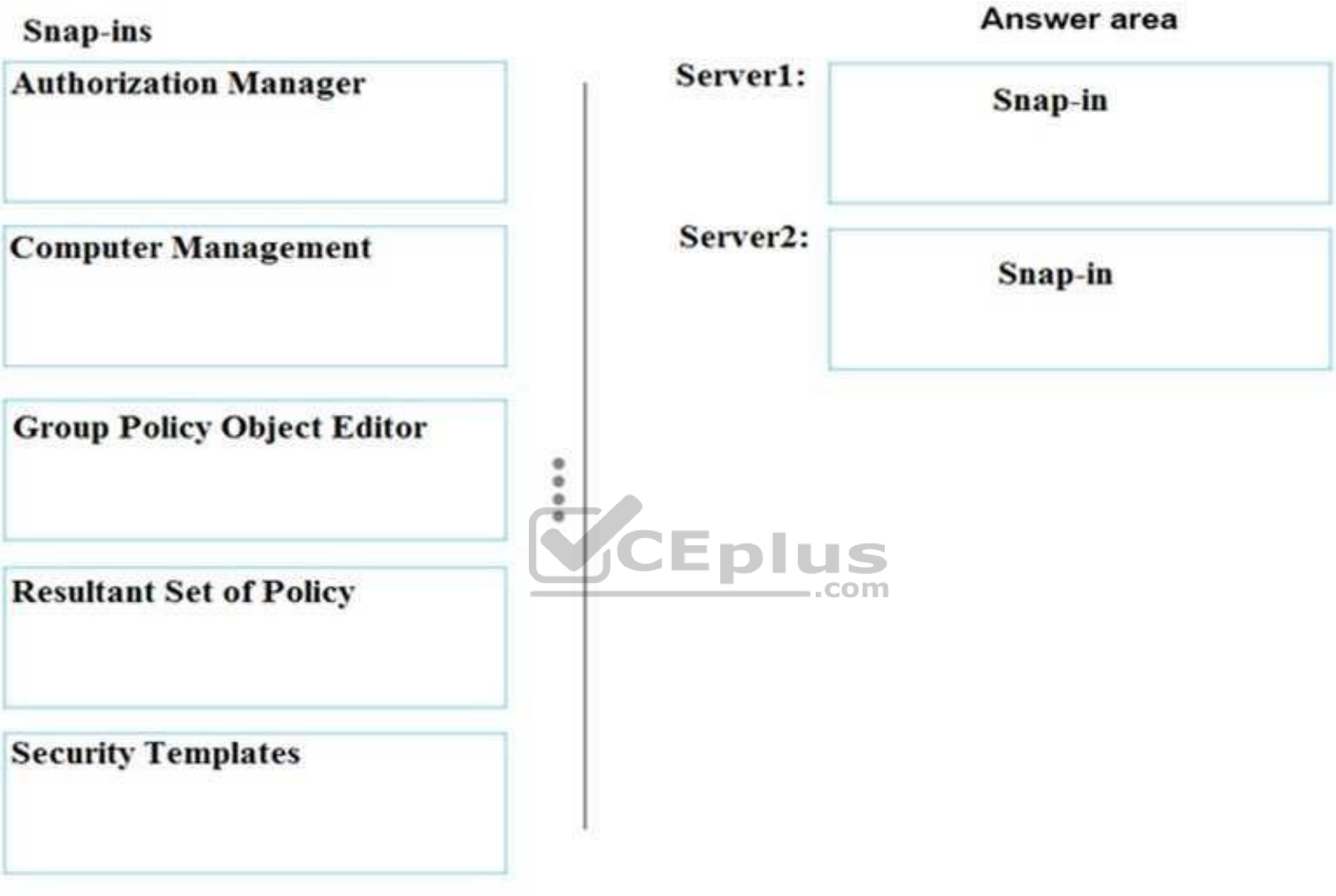
You have two servers named Server1 and Server2 that run Windows Server 2016. The servers are in a workgroup.

You need to create a security template that contains the security settings of Server1 and to apply the template to Server2. The solution must minimize administrative effort.

Which snap-in should you use for each server? To answer, drag the appropriate snap-ins to the correct servers. Each snap-in may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Snap-ins

Authorization Manager

Computer Management

Group Policy Object Editor

Resultant Set of Policy

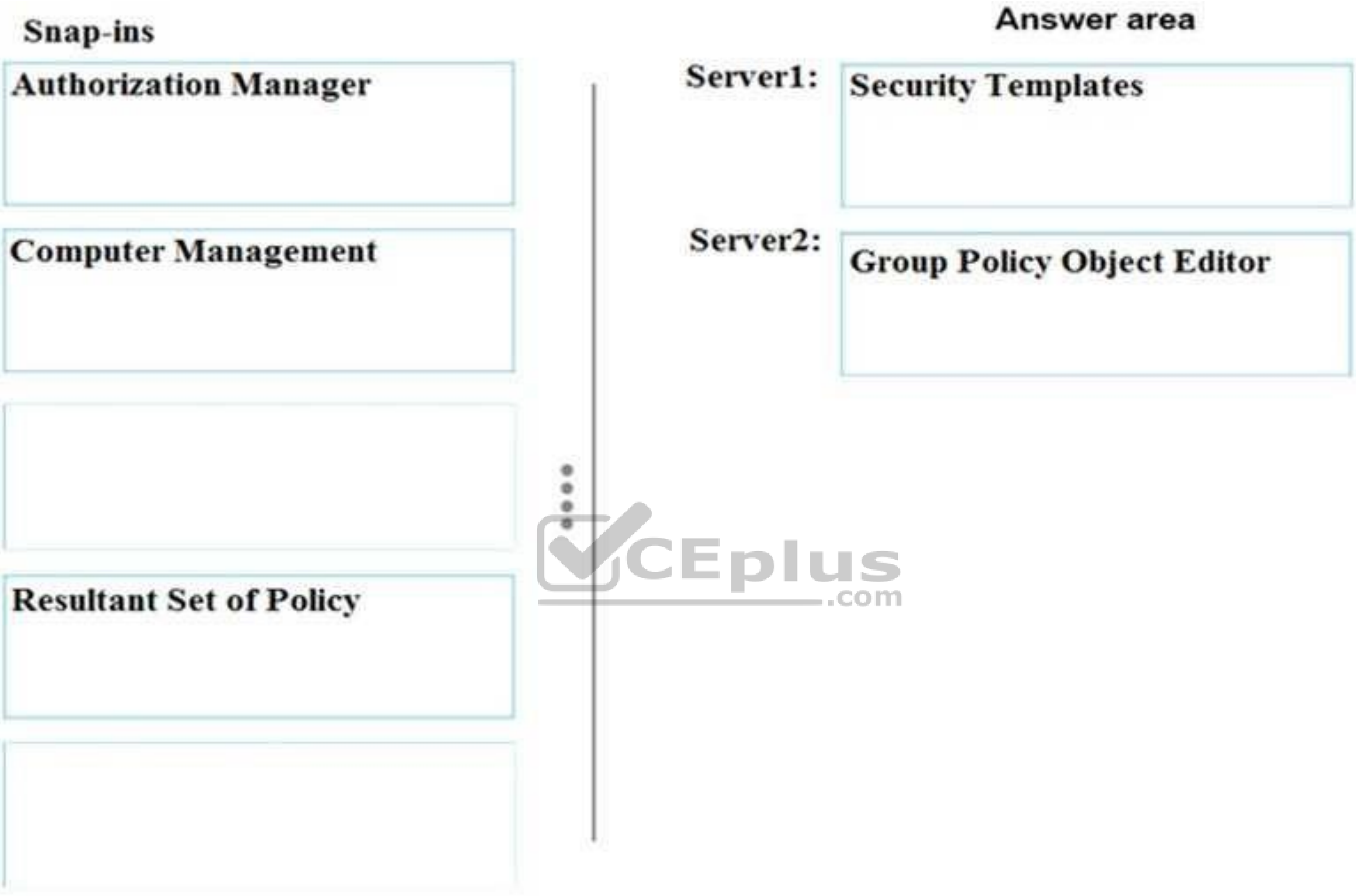
Security Templates

Answer area

Server1: Snap-in

Server2: Snap-in

Correct Answer:



Snap-ins

Authorization Manager

Computer Management

Resultant Set of Policy

Answer area

Server1: Security Templates

Server2: Group Policy Object Editor

Section: (none)
Explanation

Explanation/Reference:

References: https://www.windows-server-2012-r2.com/security-templates.html **QUESTION 40**

You are creating a Nano Server image for the deployment of 10 servers.

You need to configure the servers as guarded hosts that use Trusted Platform Module (TPM) attestation.

Which three packages should you include in the Nano Server image? Each correct answer presents part of the solution.

A. Microsoft-NanoServer-SCVMM-Compute-Package
B. Microsoft-NanoServer-SecureStartup-Package
C. Microsoft-NanoServer-Compute-Package
D. Microsoft-NanoServer-ShieldedVM-Package
E. Microsoft-NanoServer-Storage-Package
F. Microsoft-NanoServer-SCVMM- Package

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/system-center/vmm/guarded-deploy-host?toc=/windows-server/virtualization/ https://docs.microsoft.com/en-us/windows-server/get-started/deploy-nano-server

QUESTION 41
Your network contains an Active Directory domain named contoso.com. The domain contains several shielded virtual machines.

You deploy a new server named Server1 that runs Windows Server 2016.

You install the Hyper-V server role on Server1.

You need to ensure that you can host shielded virtual machines on Server1.

What should you install on Server1?

A. Host Guardian Hyper-V Support
B. the Windows Biometric Framework (WBF)
C. VM Shielding Tools for Fabric Management
D. BitLocker Network Unlock

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabricguarded-host-prerequisites

QUESTION 42
Your network contains an Active Directory domain named contoso.com.

You deploy a server named Server1 that runs Windows Server 2016. Server1 is in a workgroup.

You need to collect the logs from Server1 by using Log Analytics in Microsoft Operations Management Suite (OMS).

What should you do first?

A. Create an event subscription
B. Create a Data Collector-Set
C. Install Microsoft Monitoring Agent on Server1
D. Join Server1 to the domain

Correct Answer: C
Section: (none)
Explanation

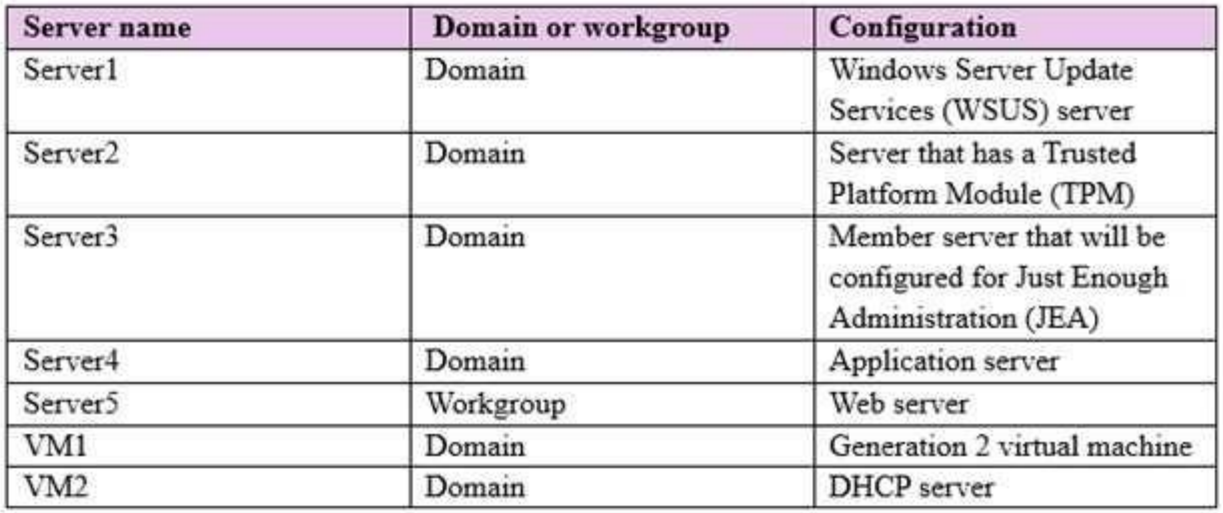
Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents

QUESTION 43
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario.

Your company has a marketing department.

The network contains an Active Directory domain named constoso.com. The domain contains the servers configured as shown in the following table.



Server name	Domain or workgroup	Configuration
Server1	Domain	Windows Server Update Services (WSUS) server
Server2	Domain	Server that has a Trusted Platform Module (TPM)
Server3	Domain	Member server that will be configured for Just Enough Administration (JEA)
Server4	Domain	Application server
Server5	Workgroup	Web server
VM1	Domain	Generation 2 virtual machine
VM2	Domain	DHCP server

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members. All laptops are protected by using BitLocker Drive Encryption (BitLocker).

You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers. An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1. A GPO named GP2 is linked to OU2.

All computers receive updated from Server1. You create an update rule named Update1.

End of repeated scenario.

You enable deep script block logging for Windows PowerShell.

In which event log will PowerShell code that is generated dynamically appear?

A. Applications and Services Logs/Windows PowerShell
B. Windows Logs/Security
C. Applications and Services Logs/Microsoft/Windows/PowerShell/Operational
D. Windows Logs/Application

Correct Answer: C
Section: (none)

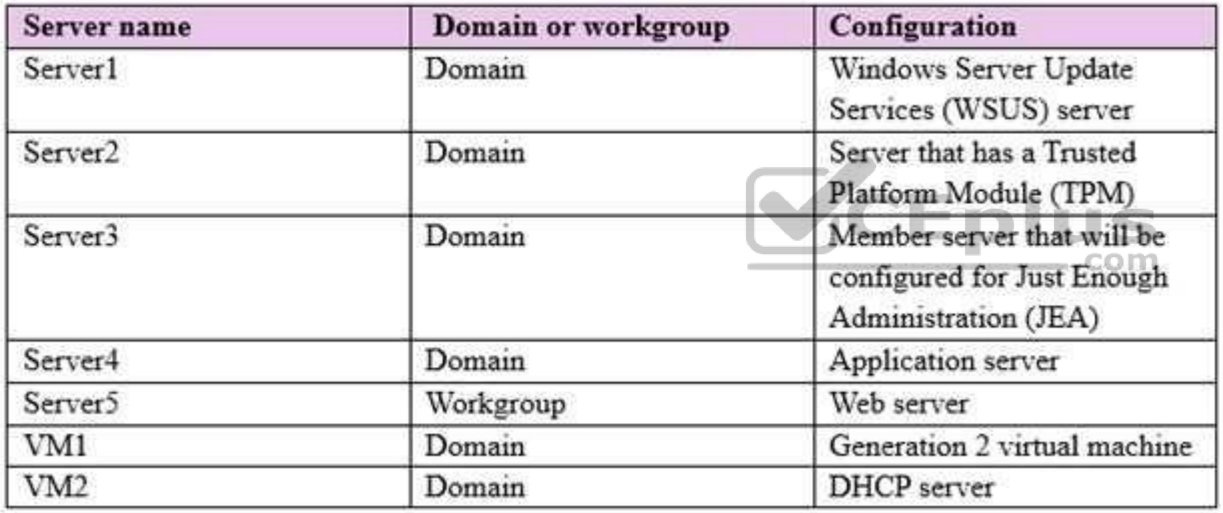
Explanation
Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script

QUESTION 44
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario.

Your company has a marketing department.

The network contains an Active Directory domain named constoso.com. The domain contains the servers configured as shown in the following table.



Server name	Domain or workgroup	Configuration
Server1	Domain	Windows Server Update Services (WSUS) server
Server2	Domain	Server that has a Trusted Platform Module (TPM)
Server3	Domain	Member server that will be configured for Just Enough Administration (JEA)
Server4	Domain	Application server
Server5	Workgroup	Web server
VM1	Domain	Generation 2 virtual machine
VM2	Domain	DHCP server

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members. All laptops are protected by using BitLocker Drive Encryption (BitLocker).

You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers. An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1. A GPO named GP2 is linked to OU2.

All computers receive updated from Server1. You create an update rule named Update1.

End of repeated scenario.

You need to create a Role Capability file on Server3. Which file should you create?

A. File1.ini
B. File1.ps1
C. File1.xml
D. File1.psrc

Correct Answer: D
Section: (none)
Explanation

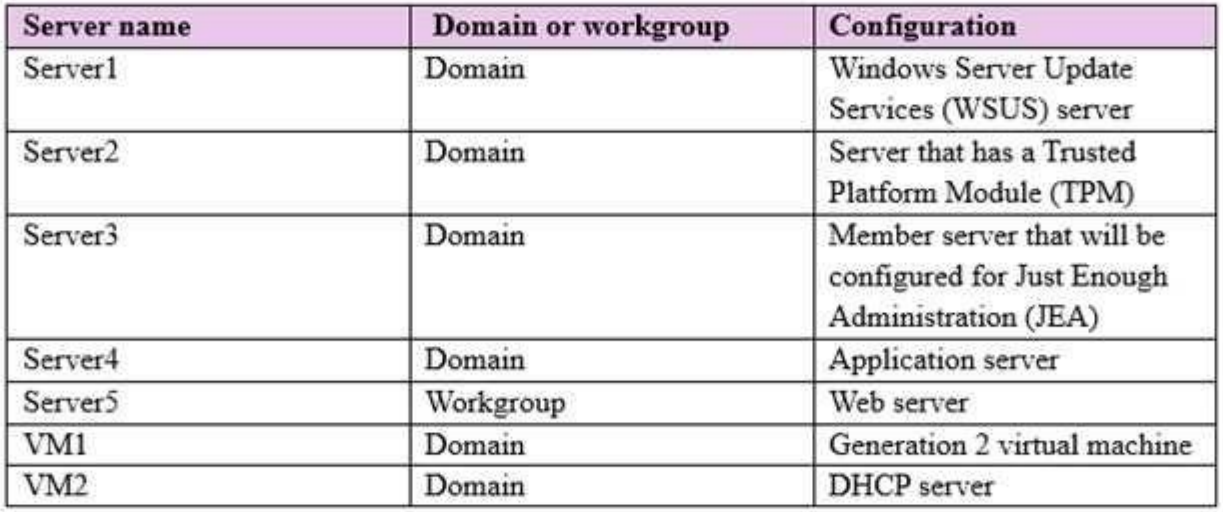
Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/jea/role-capabilities#create-a-role-capability-file

QUESTION 45
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario.

Your company has a marketing department.

The network contains an Active Directory domain named constoso.com. The domain contains the servers configured as shown in the following table.



Server name	Domain or workgroup	Configuration
Server1	Domain	Windows Server Update Services (WSUS) server
Server2	Domain	Server that has a Trusted Platform Module (TPM)
Server3	Domain	Member server that will be configured for Just Enough Administration (JEA)
Server4	Domain	Application server
Server5	Workgroup	Web server
VM1	Domain	Generation 2 virtual machine
VM2	Domain	DHCP server

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members. All laptops are protected by using BitLocker Drive Encryption (BitLocker).

You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers. An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1. A GPO named GP2 is linked to OU2.

All computers receive updated from Server1.

You create an update rule named Update1.

End of repeated scenario.

You need to implement BitLocker Network Unlock for all of the laptops. Which server role should you deploy to the network?

A. Host Guardian Service
B. Device Health Attestation
C. Windows Deployment Services
D. Network Controller

Correct Answer: C
Section: (none)

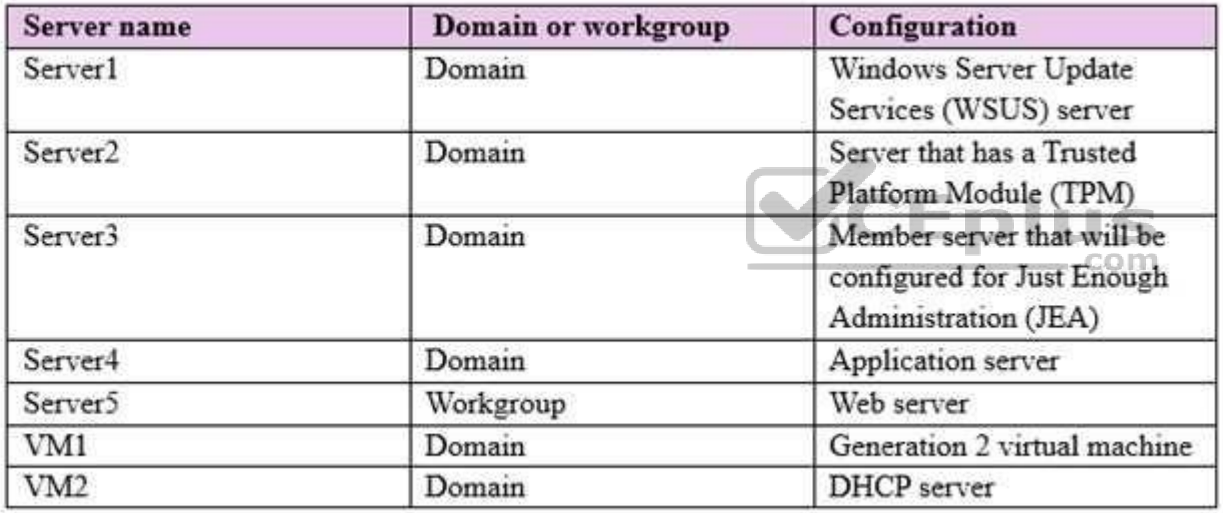
Explanation
Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-how-to-enable-network-unlock

QUESTION 46
Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario.

Your company has a marketing department.

The network contains an Active Directory domain named constoso.com. The domain contains the servers configured as shown in the following table.



Server name	Domain or workgroup	Configuration
Server1	Domain	Windows Server Update Services (WSUS) server
Server2	Domain	Server that has a Trusted Platform Module (TPM)
Server3	Domain	Member server that will be configured for Just Enough Administration (JEA)
Server4	Domain	Application server
Server5	Workgroup	Web server
VM1	Domain	Generation 2 virtual machine
VM2	Domain	DHCP server

All servers run Windows Server 2016. All client computers run Windows 10 and are domain members. All laptops are protected by using BitLocker Drive Encryption (BitLocker).

You have an organizational unit (OU) named OU1 that contains the computer accounts of application servers. An OU named OU2 contains the computer accounts of the computers in the marketing department. A Group Policy object (GPO) named GP1 is linked to OU1. A GPO named GP2 is linked to OU2.

All computers receive updated from Server1. You create an update rule named Update1.

End of repeated scenario.

You need to ensure that AppLocker rules will apply to the marketing department computers. What should you do?

A. From the properties of OU2, modify the COM+ partition Set.
B. In GP2, configure the Startup type for the Application Identity service.
C. In GP2, configure the Startup type for the Application Management service.
D. From the properties of OU2, modify the Security settings.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/device-security/applocker/configure-the-application-identity-service

QUESTION 47
Your network contains an Active Directory domain named contoso.com. The domain contains a certification authority (CA).

You need to implement code integrity policies and sign them by using certificates issued by the CA.

You plan to use the same certificate to sign policies on multiple computers.

You duplicate the Code Signing certificate template and name the new template CodeIntegrity.

How should you configure the CodeIntegrity template?

A. Enable the Allow private key to be exported setting and modify the Key Usage extension.
B. Disable the Allow private key to be exported setting and modify the Application Policies extension.
C. Disable the Allow private key to be exported setting and disable the Basic Constraints extension.
D. Enable the Allow private key to be exported setting and enable the Basic Constraints extension

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://blogs.technet.microsoft.com/ukplatforms/2017/05/04/create-code-integrity-signing-certificate/

QUESTION 48
Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.

You deploy the Local Administrator Password Solution (LAPS) to the network.

You discover that the members of a group named FinanceAdministartors can view the password of the local Administrator accounts on the servers in an organizational unit (OU) named FinanceServers.

You need to prevent the FinanceAdministartors members from viewing the local administrators ‘passwords on the servers in FinanceServers. Which permission should you remove from FinanceAdministartors?

A. all extended rights
B. read all properties
C. read permissions
D. list contents

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://4sysops.com/archives/set-up-microsoft-laps-local-administrator-password-solution-in-active-directory/

QUESTION 49
Your network contains an Active Directory Domain named contoso.com. The domain contains 10 servers hat run Windows Server 2016 and 800 client computers that run Windows 10.

You need to configure the domain to meet the following requirements:

Users must be locked out from their computer if they enter an incorrect password twice.
Users must only be able to unlock a locked account by using a one-time password that is sent to their mobile phone.

You deploy all the components of Microsoft Identity Manager (MIM) 2016.

Which three actions should you perform before you deploy the MIM add-ins and extensions? Each correct answer presents part of the solution.

A. Deploy a Multi-Factor Authentication provider and copy the required certificates to the MIM server.
B. From a Group Policy object (GPO), configure Public Key Policies.
C. From the MIM Portal, configure the Owner Approval Workflow.
D. Deploy a Multi-Factor Authentication provider and copy the required certificates to the client computers.
E. From the MIM Portal, configure the Password Reset AuthN Workflow.

F. From a Group Policy object (GPO), configure Security Settings.

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/microsoft-identity-manager/working-with-self-service-password-reset

QUESTION 50
You have a file server named FS1 that runs Windows Server 2016.

You plan to disable SMB 1.0 on the server.

You need to verify which computers access FS1 by using SMB 1.0.

What should you run first?

A. **Debug-FileShare**
B. **Set-FileShare**
C. **Set-SmbShare**
D. **Set-SmbServerConfiguration**
E. **Set-SmbClientConfiguration**

Correct Answer: D
Section: (none)
Explanation

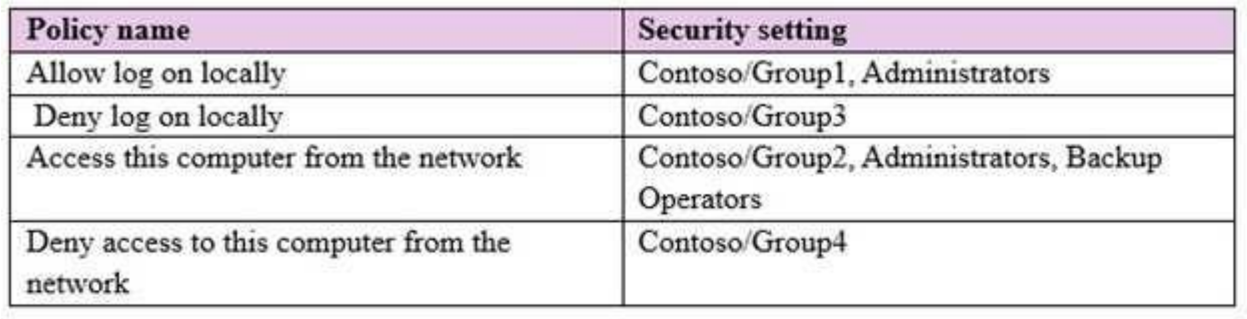
Explanation/Reference:

QUESTION 51
Your network contains an Active Directory domain named contoso.com.

The domain contains four global groups named Group1, Group2, Group3, and Group4. A user named User1 is a member of Group3.

You have an organizational unit (OU) named OU1 that contains computer accounts. A Group Policy object (GPO) named GPO1 is linked to OU1. OU1 contains a computer account named Computer1.

GPO1 has the User Rights Assignment configured as shown in the following table.



Policy name	Security setting
Allow log on locally	Contoso/Group1, Administrators
Deny log on locally	Contoso/Group3
Access this computer from the network	Contoso/Group2, Administrators, Backup Operators
Deny access to this computer from the network	Contoso/Group4

You need to ensure that User1 can access the shares on Computer1. What should you do?

A. Modify the membership of Group3. B.
Modify the membership of Group2. C.
Modify the membership of Group1.
D. Modify the membership of Group4.

Correct Answer: B
Section: (none)
Explanation

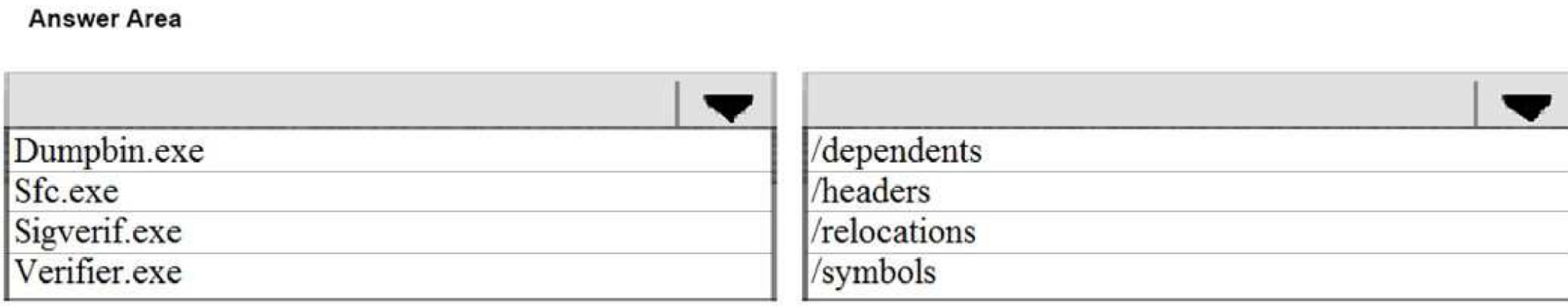
Explanation/Reference:

QUESTION 52
HOTSPOT

Your network contains an Active Directory domain named contoso.com.

You plan to deploy an application named App1.exe.

You need to verify whether Control Flow Guard is enabled for App1.exe.

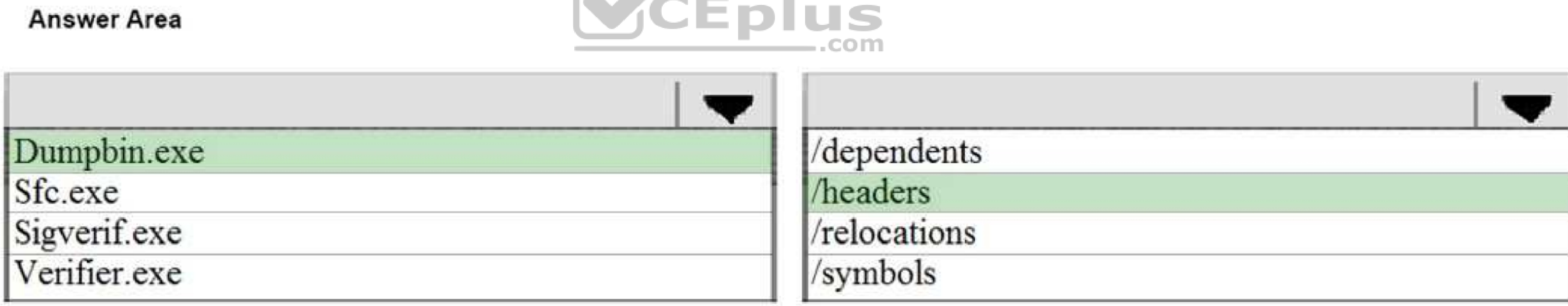


Answer Area

- Dumpbin.exe
- Sfc.exe
- Sigverif.exe
- Verifier.exe

- /dependents
- /headers
- /relocations
- /symbols

Which command should you run? To answer, select the appropriate options in the answer area.



Answer Area

- [✓ Dumpbin.exe]
- Sfc.exe
- Sigverif.exe
- Verifier.exe

- /dependents
- [✓ /headers]
- /relocations
- /symbols

Hot Area:
Correct Answer:

Section: (none)
Explanation

Explanation/Reference:
Explanation:

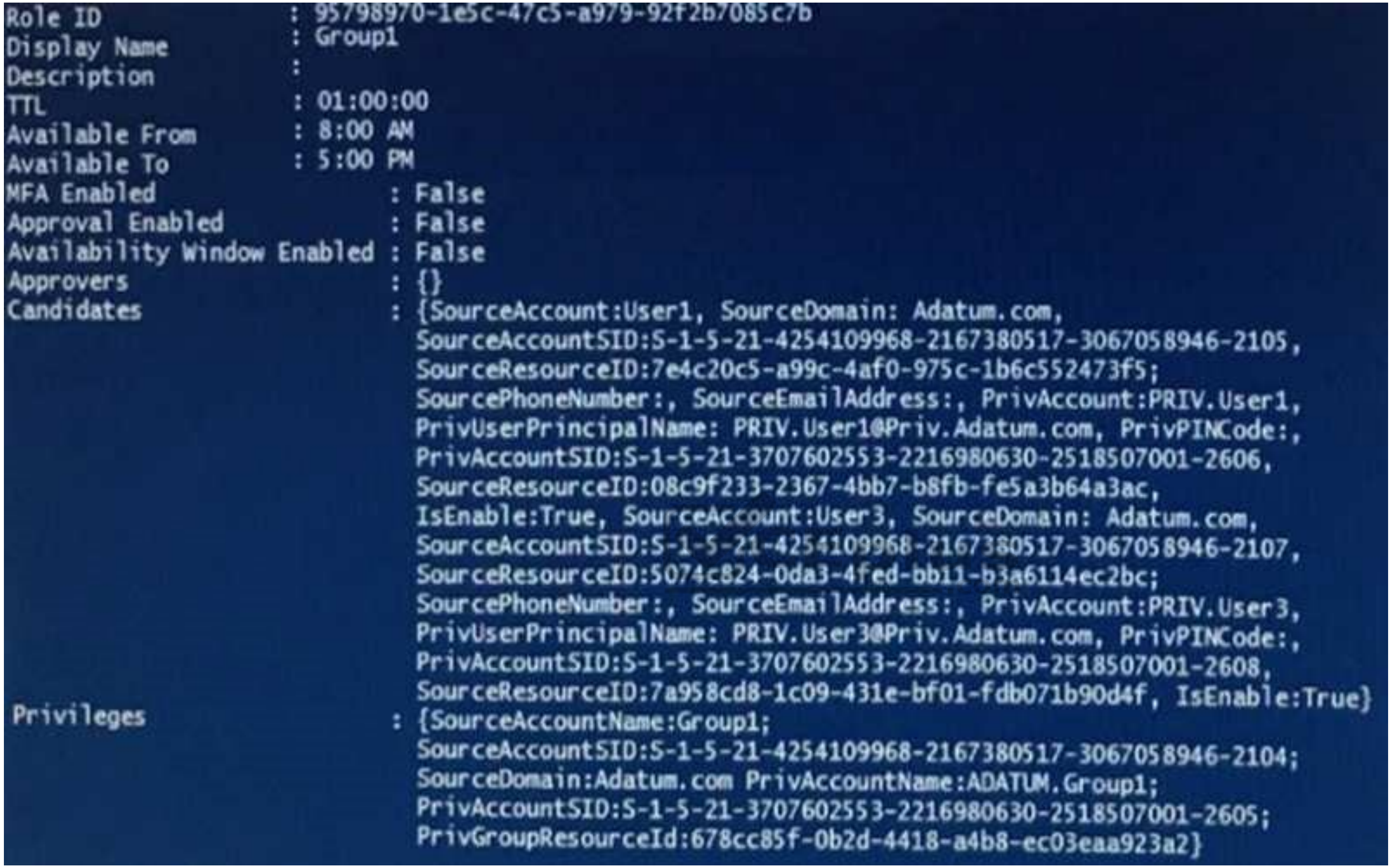
References: https://msdn.microsoft.com/en-us/library/windows/desktop/mt637065(v=vs.85).aspx

QUESTION 53
HOTSPOT

Your network contains two Active Directory forests named adatum.com and priv.adatum.com.

You deploy Microsoft Identity Manager (MIM) 2016 to the priv.adatum.com domain, and you implement Privileged Access Management (PAM).

You create a PAM role named Group1 as shown in the following exhibit.

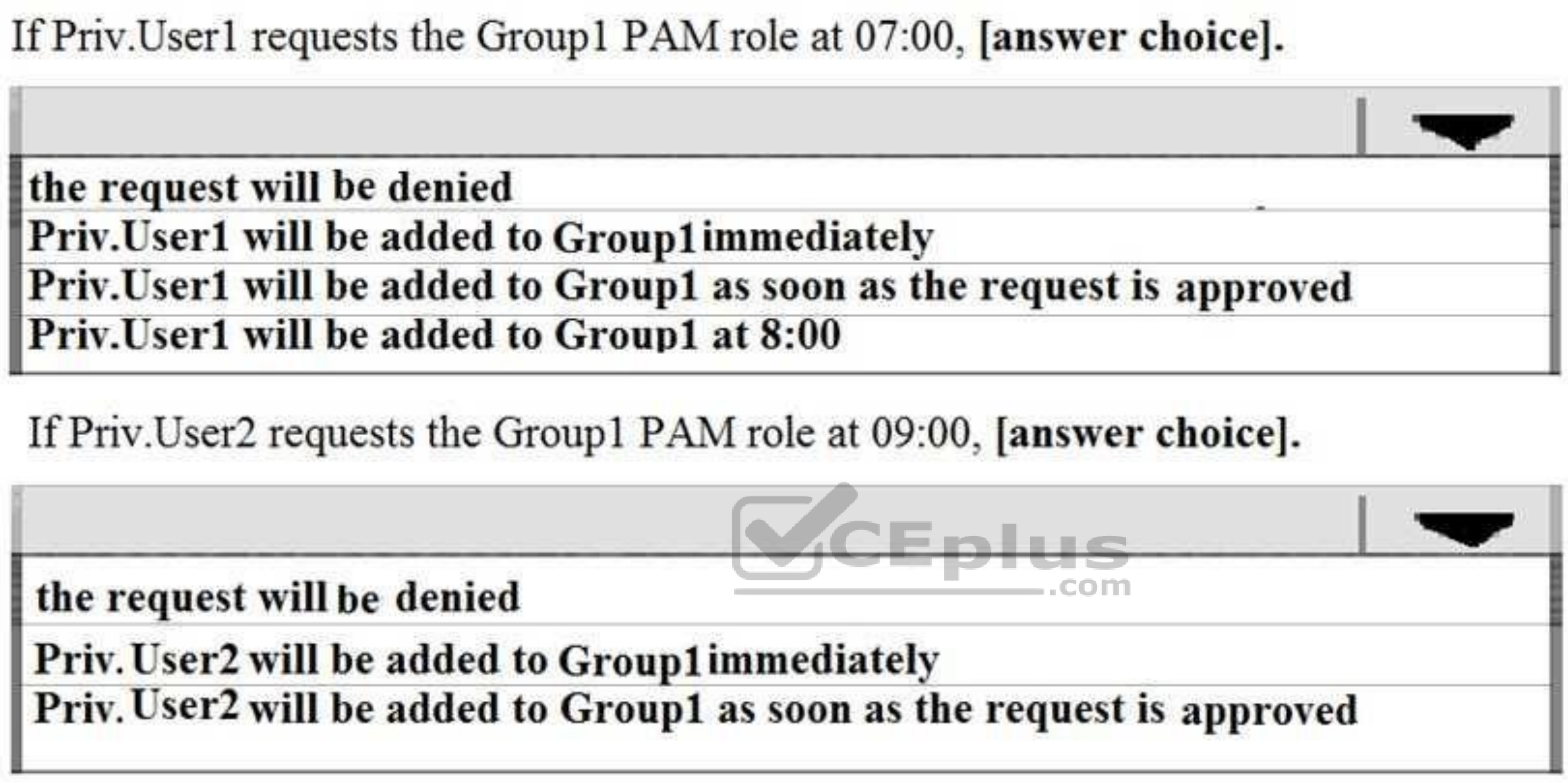


```
Role ID                  : 95798970-1e5c-47c5-a979-92f2b7085c7b
Display Name             : Group1
Description              :
TTL                      : 01:00:00
Available From           : 8:00 AM
Available To             : 5:00 PM
MFA Enabled                        : False
Approval Enabled                   : False
Availability Window Enabled        : False
Approvers                          : {}
Candidates                         : {SourceAccount:User1, SourceDomain: Adatum.com,
                                     SourceAccountSID:S-1-5-21-4254109968-2167380517-3067058946-2105,
                                     SourceResourceID:7e4c20c5-a99c-4af0-975c-1b6c552473f5;
                                     SourcePhoneNumber:, SourceEmailAddress:, PrivAccount:PRIV.User1,
                                     PrivUserPrincipalName: PRIV.User1@Priv.Adatum.com, PrivPINCode:,
                                     PrivAccountSID:S-1-5-21-3707602553-2216980630-2518507001-2606,
                                     SourceResourceID:08c9f233-2367-4bb7-b8fb-fe5a3b64a3ac,
                                     IsEnable:True, SourceAccount:User3, SourceDomain: Adatum.com,
                                     SourceAccountSID:S-1-5-21-4254109968-2167380517-3067058946-2107,
                                     SourceResourceID:5074c824-0da3-4fed-bb11-b3a6114ec2bc;
                                     SourcePhoneNumber:, SourceEmailAddress:, PrivAccount:PRIV.User3,
                                     PrivUserPrincipalName: PRIV.User3@Priv.Adatum.com, PrivPINCode:,
                                     PrivAccountSID:S-1-5-21-3707602553-2216980630-2518507001-2608,
                                     SourceResourceID:7a958cd8-1c09-431e-bf01-fdb071b90d4f, IsEnable:True}
 Privileges                        : {SourceAccountName:Group1;
                                     SourceAccountSID:S-1-5-21-4254109968-2167380517-3067058946-2104;
                                     SourceDomain:Adatum.com PrivAccountName:ADATUM.Group1;
                                     PrivAccountSID:S-1-5-21-3707602553-2216980630-2518507001-2605;
                                     PrivGroupResourceId:678cc85f-0b2d-4418-a4b8-ec03eaa923a2}
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

Hot Area:

Answer Area



If Priv.User1 requests the Group1 PAM role at 07:00, **[answer choice].**

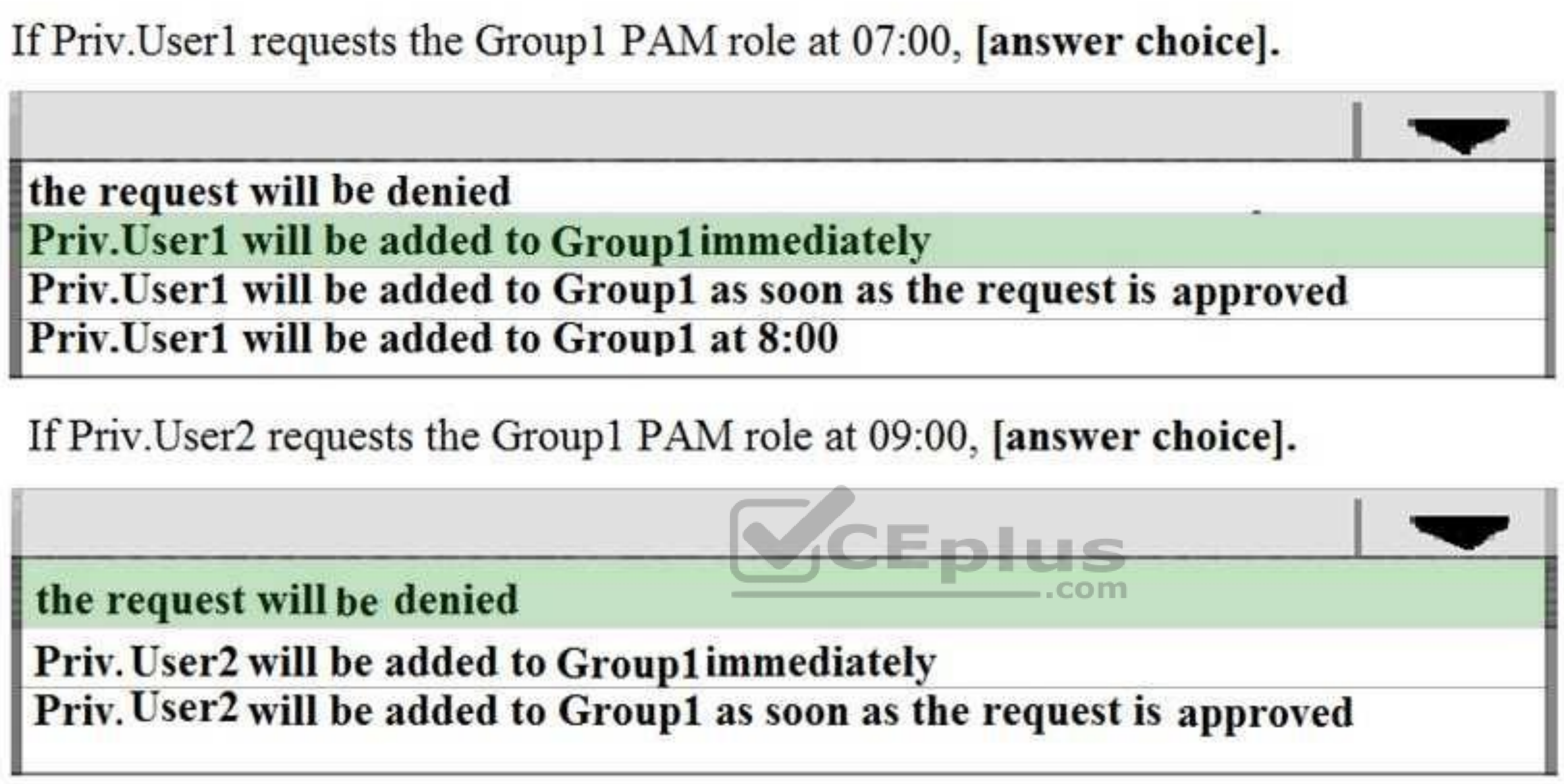
- the request will be denied
- Priv.User1 will be added to Group1 immediately
- Priv.User1 will be added to Group1 as soon as the request is approved
- Priv.User1 will be added to Group1 at 8:00

If Priv.User2 requests the Group1 PAM role at 09:00, **[answer choice].**

- the request will be denied
- Priv. User2 will be added to Group1 immediately
- Priv. User2 will be added to Group1 as soon as the request is approved

Correct Answer:

Answer Area



If Priv.User1 requests the Group1 PAM role at 07:00, **[answer choice].**

- the request will be denied
- [✓ Priv.User1 will be added to Group1immediately]
- Priv.User1 will be added to Group1 as soon as the request is approved
- Priv.User1 will be added to Group1 at 8:00

If Priv.User2 requests the Group1 PAM role at 09:00, **[answer choice].**

- [✓ the request will be denied]
- Priv. User2 will be added to Group1immediately
- Priv. User2 will be added to Group1 as soon as the request is approved

Section: (none)
Explanation

Explanation/Reference:
Explanation:
References:https://tlktechidentitythoughts.wordpress.com/2016/09/07/mim-2016-setting-up-privileged-access-management-pam-in-an-existing-domain-using-thebuilt-in-pam-tool/

QUESTION 54

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. The domain has Dynamic Access Control enabled.

Server1 contains a folder named C:\Folder1. Folder1 is shared as Share1.

You need to audit all access to the contents of Folder1 from Server2. The solution must minimize the number of event log entries.

Which two audit policies should you enable on Server1? Each correct answer presents part of the solution.

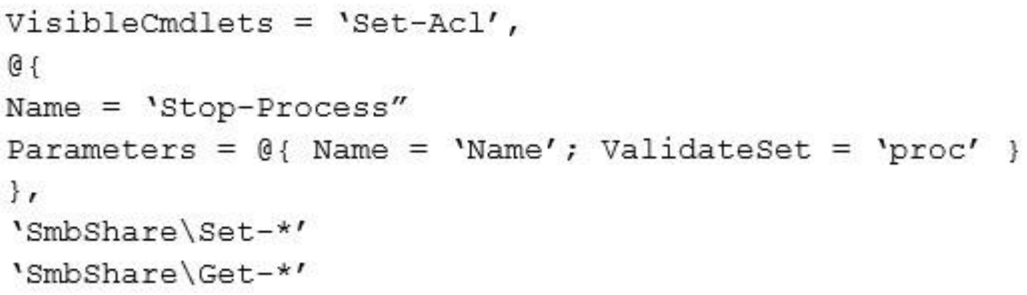
NOTE: Each correct selection is worth one point.

A. Global Object Access- File System
B. Object Access – Audit Detailed File Share
C. Object Access – Audit Other Object Access Events
D. Object Access – Audit File System
E. Object Access – Audit File Share

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-detailed-file-share https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-file-share

QUESTION 55
You implement Just Enough Administration (JEA) on several file servers that run Windows Server 2016. The Role Capability file from a server named Server5 contains the following code.



```
VisibleCmdlets = ‘Set-Acl’,
@{
Name = ‘Stop-Process”
Parameters = @{ Name = ‘Name’; ValidateSet = ‘proc’ }
},
‘SmbShare\Set-*’
‘SmbShare\Get-*’
```

Which action can be performed by a user who connects to Server5?

A. View the NTFS permissions of any folder.
B. Stop any process.
C. Create a new file share.
D. Modify the properties of any share.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/jea/role-capabilities https://technet.microsoft.com/en-us/itpro/powershell/windows/smbshare/set-smbshare

QUESTION 56
Your network contains an Active Directory domain named contoso.com. The domain contains 10 computers that are in an organizational unit (OU) named OU1.

You deploy the Local Administrator Password Solution (LAPS) client to the computers. You link a Group Policy object (GPO) named GPO1 to OU1, and you configure the LAPS password policy settings in GPO1.

You need to ensure that the administrator passwords on the computers in OU1 are managed by using LAPS.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Enable LDAP encryption on the domain controllers.
B. Restart the computers.

C. Modify the permissions on OU1.
D. Restart the domain controller that hosts the PDC emulator role.
E. Update the Active Directory Schema.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
References: https://www.techrepublic.com/article/pro-tip-securing-windows-local-administrator-password-with-laps/

QUESTION 57
Your network contains an Active Directory forest named corp.contoso.com.

You are implementing Privileged Access Management (PAM) by using a bastion forest named priv.contoso.com.

You need to create shadow groups in priv.contoso.com.

Which cmdlet should you use?

A. **New-RoleGroup**
B. **New-PamRole**
C. **New-ADGroup**
D. **New-PamGroup**

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/identitymanager/mimpam/vlatest/new-pamgroup

QUESTION 58
Your network contains an Active Directory forest named contoso.com. The forest contains three domains. All domain controllers run Windows Server 2016.

You deploy a second Active Directory forest named admin.contoso.com. The forest contains a domain member server named Server1. Server1 has Microsoft Identity Manager (MIM) 2016 deployed.

You need to implement Privileged Access Management (PAM) and to use admin.contoso.com as an administrative forest.

Which two actions should you perform? Each correct answer presents part of the solution.

A. From Server1, run the **New-PAMTrust** cmdlet.

B. From a domain controller in contoso.com, run the **New-PAMDomainConfiguration** cmdlet.
C. From a domain controller in admin.contoso.com, run the **New-PAMTrust** cmdlet.
D. From a domain controller in contoso.com, run the **New-PAMTrust** cmdlet.
E. From a domain controller in admin.contoso.com, run the **New-PAMDomainConfiguration** cmdlet.
F. From Server1, run the **New- PAMDomainConfiguration** cmdlet.

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/configuring-mim-environment-for-pam https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/step-5-establish-trust-between-priv-corpforests

QUESTION 59
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows10.

The network uses the 172.16.0.0/16 address space.

Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.

You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.

Solution: You run the **New-NetFirewallRule -DisplayName "Rule1" -Direction Inbound -LocalPort 8080 -Protocol TCP -Action Allow -Profile Domain** command.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 60
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows10.

The network uses the 172.16.0.0/16 address space.

Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.

You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.

Solution: You configure an inbound rule that allows the TCP protocol on port 8080, uses a scope of 172.16.0.0/16 for local IP addresses, and applies to a private profile.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd448531(v=ws.10)

QUESTION 61

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows10.

The network uses the 172.16.0.0/16 address space.

Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.

You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.

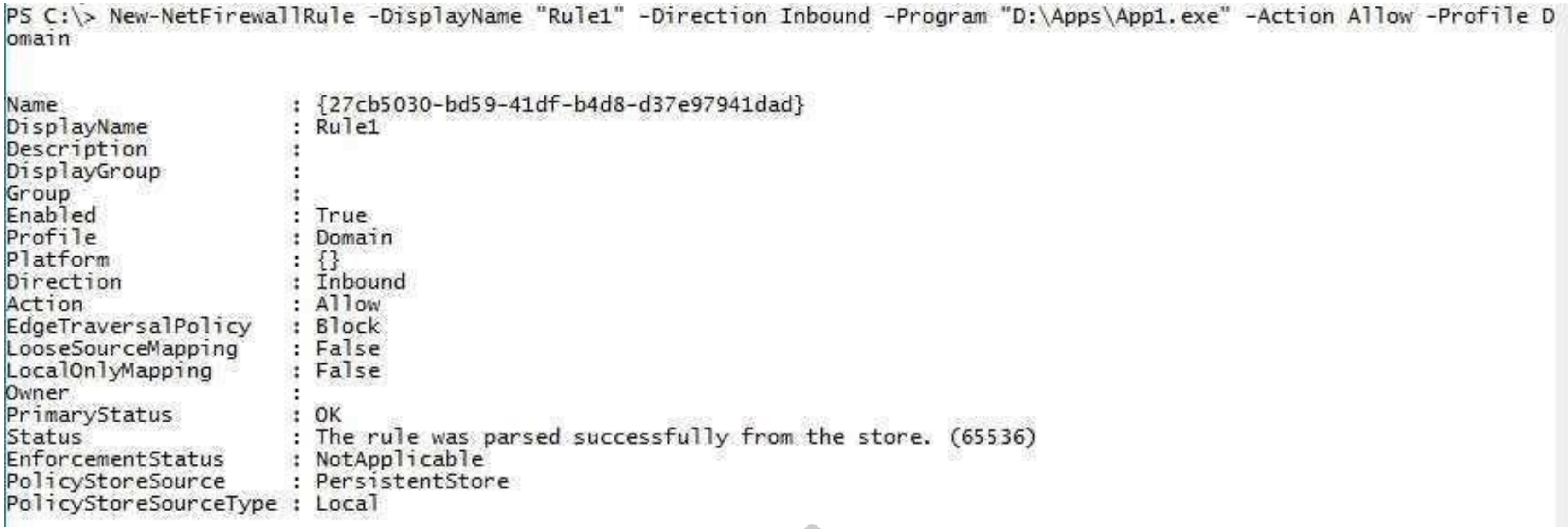
Solution: You run the **New-NetFirewallRule –DisplayName "Rule1" –Direction Inbound –Program "D:\Apps\App1.exe" –Action Allow -Profile Domain** command.

Does this meet the goal?

A. Yes
B. No

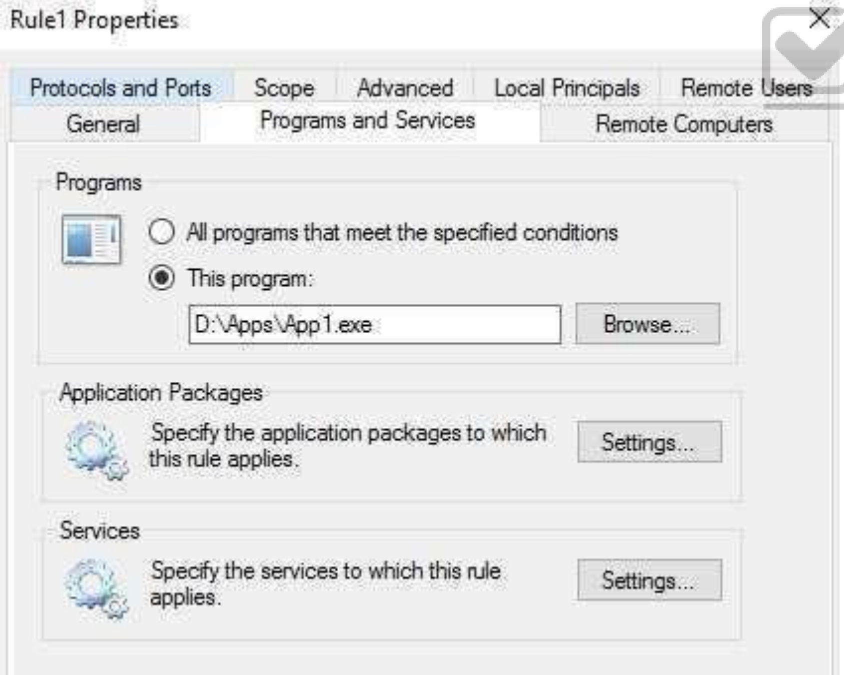
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:



```
PS C:\> New-NetFirewallRule -DisplayName "Rule1" -Direction Inbound -Program "D:\Apps\App1.exe" -Action Allow -Profile D
omain


Name                  : {27cb5030-bd59-41df-b4d8-d37e97941dad}
DisplayName           : Rule1
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Domain
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```



Programs

○ All programs that meet the specified conditions

● This program:

D:\Apps\App1.exe

Application Packages

Specify the application packages to which this rule applies.

Services

Specify the services to which this rule applies.

QUESTION 62

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016.

You need to prevent NTLM authentication on Server1.

Solution: From a Group Policy, you configure the Kerberos Policy.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

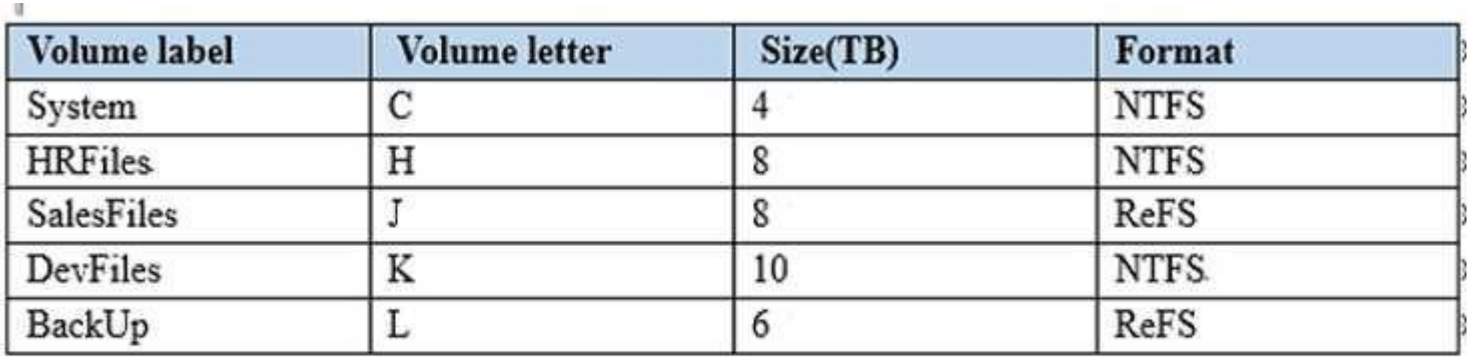
Explanation/Reference:
References: https://www.rootusers.com/implement-ntlm-blocking-in-windows-server-2016/

QUESTION 63

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.



Volume label	Volume letter	Size(TB)	Format
System	C	4	NTFS
HRFiles	H	8	NTFS
SalesFiles	J	8	ReFS
DevFiles	K	10	NTFS
BackUp	L	6	ReFS

You need to encrypt DevFiles by using BitLocker Drive Encryption (ButLocker).

Solution: You run the **Lock-BitLocker** cmdlet.

Does this meet the goal?

A. Yes
B. No

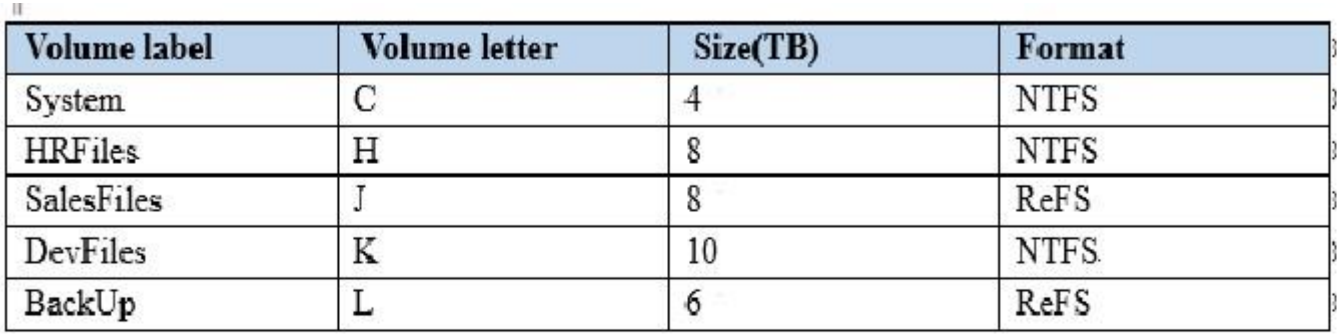
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/bitlocker/lock-bitlocker?view=win10-ps

QUESTION 64
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.



Volume label	Volume letter	Size(TB)	Format
System	C	4	NTFS
HRFiles	H	8	NTFS
SalesFiles	J	8	ReFS
DevFiles	K	10	NTFS
BackUp	L	6	ReFS

You need to encrypt DevFiles by using BitLocker Drive Encryption (ButLocker).

Solution: You run the **manage-bde.exe** command and specify the –*on* parameter.

Does this meet the goal?

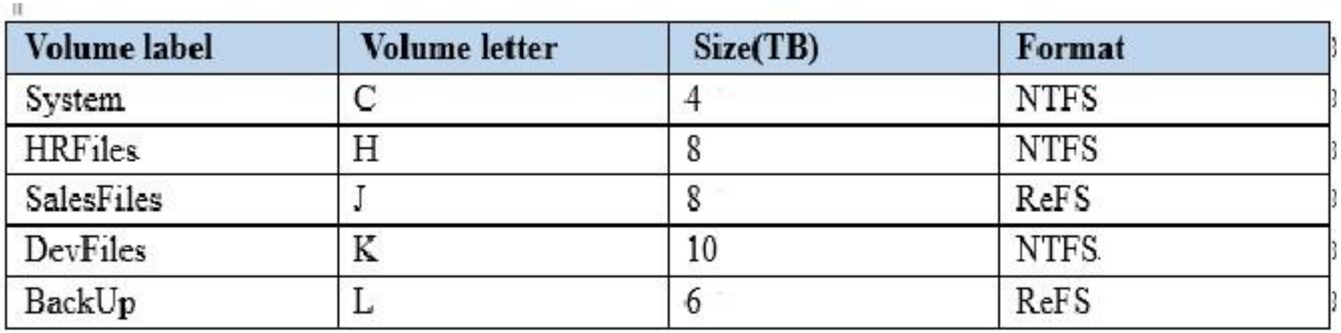
A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/manage-bde-on

QUESTION 65
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.



Volume label	Volume letter	Size(TB)	Format
System	C	4	NTFS
HRFiles	H	8	NTFS
SalesFiles	J	8	ReFS
DevFiles	K	10	NTFS
BackUp	L	6	ReFS

You need to encrypt DevFiles by using BitLocker Drive Encryption (ButLocker).

Solution: You run the **Enable-BitLocker** cmdlet.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/bitlocker/enable-bitlocker?view=win10-ps

QUESTION 66
You have a guarded fabric and a Host Guardian Service server named HGS1.

You deploy a Hyper-V host named Hyper1, and configure Hyper1 as part of the guarded fabric.

You plan to deploy the first shielded virtual machine.

You need to ensure that you can run the virtual machine on Hyper1.

What should you do?

A. On HGS1, run the **Export-HgsKeyProtectionState** cmdlet, and then run the **Import-HgsGuardian** cmdlet.

B. On Hyper1, run the **Invoke-WebRequest** cmdlet, and then run the **Import-HgsGuardian** cmdlet.
C. On the virtual machine, retrieve the metadata of the guarded fabric, and then import the metadata.
D. On Hyper1, run the **Export-HgsKeyProtectionState** cmdlet, and then run the **Import-HgsGuardian** cmdlet.

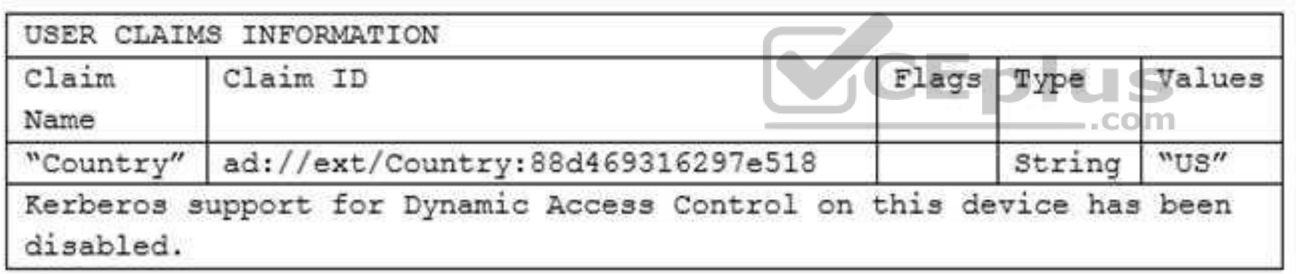
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://blogs.technet.microsoft.com/datacentersecurity/2016/06/06/step-by-step-creating-shielded-vms-without-vmm/

QUESTION 67
Your network contains an Active Directory domain named contoso.com. The domain contains domain controllers that run Windows Server 2016.

The Job Title attribute for a domain user named User1 has a value of Sales Manager.

User1 runs **whoami/claims** and receives the following output.



USER CLAIMS INFORMATION				
Claim Name	Claim ID	Flags	Type	Values
"Country"	ad://ext/Country:88d469316297e518		String	"US"
Kerberos support for Dynamic Access Control on this device has been disabled.				

You need to ensure that the security token of User1 has a claim for Job Title.

What should you do?

A. From Active Directory Users and Computers, modify the properties of the User1 account.
B. From a Group Policy object(GPO), configure KDC support for claims, compound authentication, and Kerberos armoring.
C. From Active Directory Administrative Center, add a claim type.

D. From Windows PowerShell, run the **New-ADClaimTransformPolicy** cmdlet and specify the *–Name* parameter.

Correct Answer: C

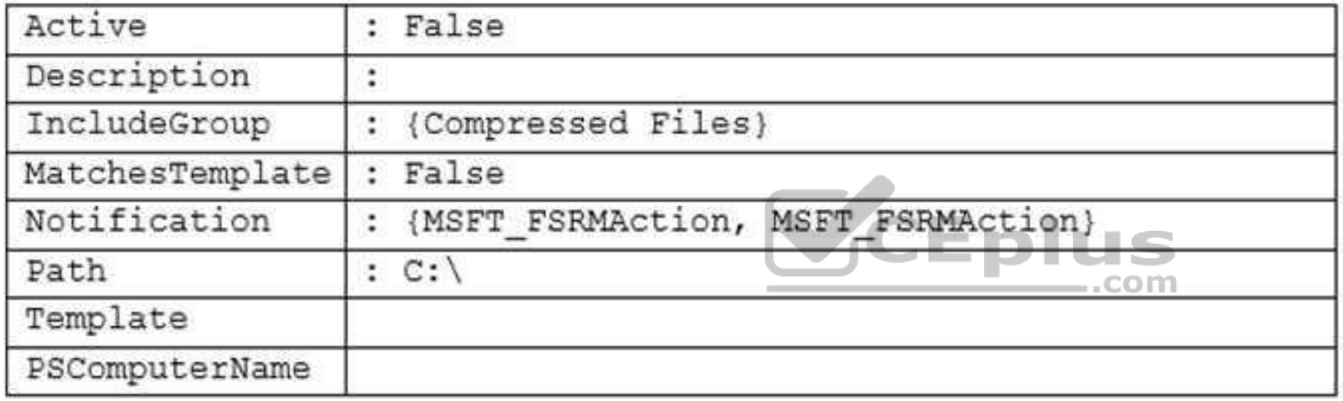
Section: (none)
Explanation

Explanation/Reference:
References: https://www.nyazit.com/how-to-configure-dynamic-access-control-in-windows-server-2012-r2-2/

QUESTION 68
You have a file server named Server1 that runs Windows Server 2016.

A new policy states that ZIP files must not be stored on Server1.

An administrator creates a file screen filter as shown in the following output.



```
Active          : False
Description     :
IncludeGroup    : {Compressed Files}
MatchesTemplate : False
Notification    : {MSFT_FSRMAction, MSFT_FSRMAction}
Path            : C:\
Template
PSComputerName
```

You need to prevent users from storing ZIP files on Server1.

What should you do?

A. Change the filter to active.
B. Enable Quota Management on all the drives.
C. Add a template to the filter.
D. Configure File System (Global Object Access Auditing).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows-server/storage/fsrm/create-file-screen

QUESTION 69
You implement Log Analytics in Microsoft Operations Management Suite (OMS) on all servers that run Windows Server 2016.

You need to generate a daily report that identifies which servers restarted during the last 24 hours.

Which query should you use?

A. EventLog:Application EventId:6009 Type:Event TimeGenerated>NOW-24HOURS
B. EventLog:System EventId:6009 Type:Event TimeGenerated>NOW+24HOURS
C. EventLog:System EventId:6009 Type:Event TimeGenerated>NOW-24HOURS
D. EventLog:Application EventId:6009 Type:Event TimeGenerated>NOW+24HOURS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Your network contains an Active Directory domain.

Microsoft Advanced Threat Analytics (ATA) is deployed to the domain.

A database administrator named DBA1 suspects that her user account was compromised.

Which three events can you identify by using ATA? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Domain computers into which DBA1 recently signed.
B. Phishing attempts that targeted DBA1.
C. The last time DBA1 experienced a failed logon attempt.

D. Spam messages received by DBA1.
E. Servers that DBA1 recently accessed.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
References: https://github.com/MicrosoftDocs/ATADocs/blob/master/ATADocs/suspicious-activity-guide.md